Computing the endomorphism ring of an abelian surface over a finite field in subexponential time

Caleb Springer

Department of Mathematics, The Pennsylvania State University

Setup

Let A be an ordinary, simple abelian variety over $\mathbb{F}_q$ of dimension 2 with Frobenius π. Write $K = \mathbb{Q}(\pi)$ and let F be the maximal totally real subfield of K.

The Problem

The endomorphism ring $\mathrm{End}(A)$ is an order in the quartic CM field K which contains $\mathbb{Z}[\pi, \overline{\pi}]$.

1. Which order $\mathcal{O} \subseteq K$ is $\mathrm{End}(A)$?
2. How do we uniquely identify this order?

Previous Work

- Bisson and Sutherland: A subexponential algorithm to compute the endomorphism ring of an ordinary elliptic curve.
- Bisson: A generalization of the elliptic curve algorithm to abelian varieties of dimension 2 whose correctness requires various heuristic assumptions.
- The algorithm presented here: A different generalization of Bisson and Sutherland's elliptic curve algorithm, which avoids the previously required heuristic assumptions.

PennState

Identifying Orders with Ideals of $\mathcal{O}_F$

- Denoting the conductor ideal of $\mathcal{O}$ by $\mathfrak{f}_{\mathcal{O}}$, there is a one-to-one correspondence (see Brooks, Jetchev and Wesolowski):

$$\underline{\text{Orders of } K \text{ containing } \mathcal{O}_F} \longleftrightarrow \underline{\text{Ideals of } \mathcal{O}_F}$$
$$\mathcal{O} \longmapsto \mathfrak{f}^+(\mathcal{O}) := \mathfrak{f}_{\mathcal{O}} \cap \mathcal{O}_F$$
$$\mathcal{O}(\mathfrak{f}^+) := \mathcal{O}_F + \mathfrak{f}^+\mathcal{O}_K \longmapsto \mathfrak{f}^+$$

- Assume A has **maximal RM**, i.e. $\mathrm{End}(A) \supseteq \mathcal{O}_F$. Then $\mathrm{End}(A)$ is identified by the ideal $\mathfrak{f}^+(\mathrm{End}(A))$. This is the output of our algorithm.
- $\mathfrak{f}^+(\mathrm{End}(A))$ divides $\mathfrak{f}^+(\mathcal{O}_F[\pi])$, so we compute $\mathfrak{f}^+(\mathrm{End}(A))$ by inspecting primes dividing $\mathfrak{f}^+(\mathcal{O}_F[\pi])$.

Determining $\mathrm{End}(A)$: The Main Idea

- Probe the ideal class group $\mathrm{Cl}(\mathrm{End}(A))$ by computing the isogenies corresponding to various ideals.
- Compare $\mathrm{Cl}(\mathrm{End}(A))$ to $\mathrm{Cl}(\mathcal{O})$ for known "testing" orders $\mathcal{O} \subseteq K$, and deduce the ideal $\mathfrak{f}^+(\mathrm{End}(A))$ which uniquely identifies the order $\mathrm{End}(A)$.
- This reduces computing $\mathrm{End}(A)$ to finding relations in various class groups $\mathrm{Cl}(\mathcal{O})$.

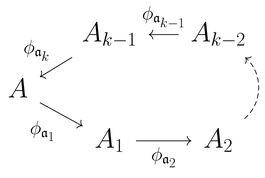
Ideal Class Group Action

The ideal class group $\mathrm{Cl}(\mathcal{O})$ acts freely on the set of abelian varieties isogenous to A with endomorphism ring $\mathcal{O}$. This action is induced by associating each ideal $\mathfrak{a}$ to the isogeny $\phi_{\mathfrak{a}}$ with kernel $A[\mathfrak{a}] = \cap_{a \in \mathfrak{a}} A[a]$.

$\mathfrak{a}_1 \cdots \mathfrak{a}_k$ is trivial in $\mathrm{Cl}(\mathrm{End}(A))$

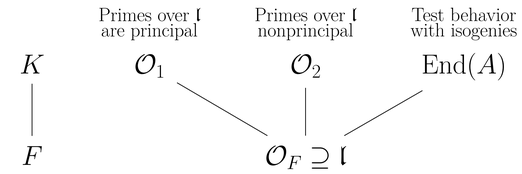
$\Updownarrow$

A is fixed by the composition $\phi_{\mathfrak{a}_k} \cdots \phi_{\mathfrak{a}_1}$



Deciding if $\mathfrak{p}^k$ Divides $\mathfrak{f}^+(\mathrm{End}(A))$

- Given prime power $\mathfrak{p}^k \subseteq \mathcal{O}_F$, construct two special "testing" orders $\mathcal{O}_1, \mathcal{O}_2 \subseteq K$. If $\mathfrak{l} \subseteq \mathcal{O}_F$ is a prime which splits into principal ideals in $\mathcal{O}_1$, but not in $\mathcal{O}_2$, then $\mathfrak{p}^k$ divides $\mathfrak{f}^+(\mathrm{End}(A))$ if and only if $\mathfrak{l}$ splits into principal ideals in $\mathrm{End}(A)$.



- **Key Proposition:** There are infinitely many such $\mathfrak{l} \subseteq \mathcal{O}_F$.
- By Chebotarev's density theorem, proving infinitely many such primes $\mathfrak{l}$ exist reduces to showing that the ring class field of $\mathcal{O}_1$ does not contain the ring class field of $\mathcal{O}_2$.

Main Result (Springer, 2018)

Using the class group action, we obtain an algorithm which is subexponential in $\log q$, as follows.

Input: Ordinary, simple abelian variety A of dimension 2 with maximal RM satisfying certain technical conditions

Output: The ideal $\mathfrak{f}^+(\mathrm{End}(A)) \subseteq \mathcal{O}_F$ which uniquely identifies $\mathrm{End}(A)$.

Heuristic Assumptions

This algorithm is unconditionally correct, except that we use a subexponential algorithm of Biasse and Fieker for finding and checking relations in the ideal class groups of various orders, which requires some standard assumptions, including GRH, to be provably correct. The running time is bounded under heuristic assumptions analogous to those used by Bisson and Sutherland in the elliptic curve case.

Restrictions

- In order to compute isogenies, we must assume A is principally polarized, F has narrow class number 1 and the conductor gap $[\mathcal{O}_F : \mathbb{Z}[\pi + \overline{\pi}]]$ is not even. See Cosset & Robert; Dudeanu et al.
- For simplicity, we assume $K \neq \mathbb{Q}(\zeta_5)$, hence $\mathcal{O}_K^* = \mathcal{O}_F^*$. Adding this assumption implies that the $\mathfrak{l}$-isogeny graphs described by Brooks, Jetchev and Wesolowski are volcanoes.